UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/965,579	09/26/2001	Linden Minnick	42390P12266	3536

8791 7590 03/14/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
03/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte LINDEN MINNICK

Appeal 2007-3985
Application 09/965,579
Technology Center 2100

Decided: March 14, 2008

Before LANCE LEONARD BARRY, JAY P. LUCAS, and STEPHEN C. SIU, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1-8, 10-19, 21, 22, 34-41, 43, and 44. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

A. Invention

11The invention at issue involves processing cryptography information (Spec. 2). Typically, a device driver receives data packets associated with security association (SA) information that contains corresponding cryptographic information (*id.*). The SA information for the data packets is contained in a single table (*id.* 3). The device driver linearly searches the table for the SA information corresponding to a received packet. However, such searches can be inefficient (*id.*).

Appellant invented a method for processing cryptography information in which SA information is stored in separate tables (i.e., transmit and receive tables) based on whether the data packet is an ingress packet or an egress packet (*Id.* 10). By splitting the SA table into separate transmit and receive tables, the efficiency of searches may be improved (*id.* 11).

B. Illustrative Claims

Claim 1, which further illustrates the invention, follows:

1. A method comprising:

receiving at a device driver a network packet having a corresponding security association (SA);

determining if the packet is an ingress packet or an egress packet;

determining for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hashing the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hashing the key value to determine a location of an entry in an egress

lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieving from the entry an index to a location of the SA in memory; and

retrieving the SA from memory based on the index.

C. REJECTIONS

Claims 1-8, 10-19, 21, 22, 34-41, 43, and 44 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,505,192 ("Godwin"), U.S. Patent No. 6,763,394 ("Tuck"), and R. Apparna & B. PremKumar, *Monitoring Ethernet Network Activity with NDIS Drivers*, California Software Laboratories White Papers, 1-2 (1999) ("Apparna"). Claims 9, 20, 31, and 42 have been cancelled. Claims 23-30, 32, and 33 have been withdrawn.

II. ISSUES AND ANALYSIS

Appellant disputes the Examiner's conclusion of obviousness of independent claims 1, 12, and 34 and argues that "the Godwin reference and the Tuck reference, whether alone or in any possible combination, fail to disclose or suggest determining whether a packet received at a device driver is an ingress or egress packet, as recited in the claimed invention" (Reply Br. 2).

The Examiner finds that although "Godwin fails to disclose determining if the packet is an ingress packet or an egress packet and the two lookup tables being separate," "Tuck teaches such limitations (see column 2 lines 29-37, column 5 lines 28-38 and claim 19)" (Ans. 6).

Based on the record before us, we do not find that Tuck discloses "determining if the packet is an ingress packet or an egress packet" as the Examiner asserts (Ans 6). Rather, Tuck discloses receiving data packets at an ingress port of a network packet router and determining if the data packet is to be passed to an egress port or dropped (col. 2, ll. 28-37 and 52-62). Tuck appears to disclose a network router having an ingress port and an egress port. However, the Examiner has not shown that Tuck discloses that the data packets received at the ingress port are determined to be ingress or egress packets and determining a location of an index to a location of security association in memory in one of an ingress lookup table or an egress lookup table based on whether the packet is an ingress or an egress packet as recited in claims 1, 12, and 34.

Therefore, we reverse the rejection of independent claims 1, 12, and 34 and of claims 2-8, 10, 11, 13-19, 21, 22, 35-41, 43, and 44, which depend therefrom.

III. ORDER

In summary, the rejection of claims 1-8, 10-19, 21, 22, 34-41, 43, and 44 under § 103(a) is reversed.

REVERSED

rwk

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040